SCOTT+SCOTT ATTORNEYS AT LAW LLP
ALEX M. OUTWATER (CA 259062)
600 W. Broadway, Suite 3300
San Diego, CA 92101
Telephone: 619-233-4565
Facsimile: 619-233-0508
aoutwater@scott-scott.com

Attorney for Plaintiff Valerie Whittaker

[Additional counsel on signature page.]

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN JOSE DIVISION

VALERIE WHITTAKER, on Behalf of Herself and All Others Similarly Situated, Plaintiff, vs. ACCELLION, INC., Defendant.	Case No. _____ **CLASS ACTION COMPLAINT** JURY TRIAL DEMANDED

Plaintiff Valerie Whittaker ("Plaintiff") brings this Class Action Complaint on behalf of herself and all others similarly situated, against Defendant**,** Accellion, Inc. ("Accellion" or "Defendant"), alleging as follows based upon information and belief and investigation of counsel, except as to the allegations specifically pertaining to her, which are based on personal knowledge:

NATURE OF THE CASE

1. This case arises out of Defendant's failure to properly maintain and store personal information. Businesses whose systems and products are designed and marketed for the purposes of storing and transferring sensitive, personally identifying information ("PII") and personal medical information[1] ("PMI") owe a duty of reasonable care to the individuals to whom that data relates.

2. Defendant owes this duty this duty to Plaintiff and the Class because it is reasonably foreseeable that the exposure of PII or PMI to unauthorized persons – and especially hackers with nefarious intentions – would result in harm to them.

3. This harm manifests in a number of ways, including identity theft and financial fraud, and the exposure of a person's PII or PMI through a data breach, which puts that person at a substantially increased and certainly impending risk of these crimes compared to the rest of the population, potentially for the rest of their lives. Mitigating that risk, to the extent it is even possible to do so, requires individuals to devote significant time and money to closely monitor their credit, financial accounts, and email accounts, and take a number of additional prophylactic measures.

4. Accellion provides cloud-based file transferring solutions to a variety of different industries, including governmental agencies, healthcare, financial services, legal, and higher education.

[1] As used herein, Plaintiff uses the term "personal medical information" to mean: individually identifiable information, in possession of or derived from a provider of health care, health care service plan, pharmaceutical company, or contractor regarding a patient's medical history, mental or physical condition, or treatment.

5. Accellion advertises safety as a major selling point for its products and services. "When employees click the Accellion button, they know it's the safe, secure way to share sensitive information with the outside world."[2] With respect to the healthcare industries, Accellion touted its platforms' ability to "provide[] secure access to sensitive content such as Electronic Health Records (EHRs) that must be protected for HIPAA compliance."[3]

6. After choosing Accellion as a file management and security provider, its clients use Accellion's products to store and transfer data that frequently includes highly sensitive PII and/or PMI.

7. Due to the nature of its business and the purposes for which Accellion marketed its products and services, Accellion knew or should have known that vulnerabilities in its products or systems would risk the exposure of consumer PII and PMI. Accellion had a resulting duty to ensure the security of its products and services.

8. Accellion's offerings include a product known as Accellion File Transfer Appliance ("FTA").

9. Unauthorized third parties exploited vulnerabilities in Accellion's FTA product in December 2020 and January 2021 to gain access to sensitive files stored or transferred using FTA by Accellion's clients (the "Data Breach").

10. Plaintiff, bring this action on behalf of herself and on behalf of classes defined herein, of individuals whose PII and PMI were accessed and exposed as a result of the Data Breach.

11. Plaintiff brings claims for actual damages, statutory damages, and punitive damages, with attorneys' fees, costs, and expenses under the California Confidentiality of Medical Information Act ("CMIA"), Cal. Civ. Code §56, *et seq.*, the California Consumer Privacy Act, Cal. Civ. Code §1798.100 *et seq.*, and further sues Defendant for negligence, negligence *per se*, unjust enrichment, and declaratory judgment pursuant to the Declaratory Judgment Act, 28 U.S.C. §2201 *et seq.*

---

[2] https://www.accellion.com/company/.

[3] Accellion, Inc., *Healthcare Data Breaches are Common, Putting Patient Data and HIPAA Compliance at Risk* (Oct. 11, 2016), *available at* https://www.accellion.com/blog/healthcare-data-breaches-are-common-putting-patient-data-and-hipaa-compliance-at-risk/.

12. The information accessed and exposed during the Data Breach was derived from hundreds of Accellion's institutional clients, involving the PII or PMI of millions of individual consumers.

13. Based on the public statements of Accellion and certain of its institutional clients to date, a wide variety of PII and PMI was implicated in the breach, including, but not limited to: names, drivers' license information, dates of birth, phone numbers, email addresses, bank account information, social security numbers, pharmacy records, and insurance information.

14. One of Accellion's customers, The Kroger Company ("Kroger"), recently confirmed that they used Accellion's services, and that some of their clinic and pharmacy customers' information was accessed and exposed during the Data Breach.

15. Since the Data Breach, more Accellion institutional clients have announced – either in public statements, notice letters, or both – that their consumers' PII and/or PMI was also compromised in the Data Breach.

16. As a direct and proximate result of Accellion's inadequate data security, Plaintiff and Class Members' PII and/or PMI has been accessed by hackers and exposed to an untold number of unauthorized individuals.

17. Plaintiff and Class Members are now at a significantly increased risk of fraud, identity theft, and similar forms of criminal mischief, which risk may last for the rest of their lives. Consequently, Plaintiff and Class Members must devote substantially more time, money, and energy protecting themselves, to the extent possible, from these crimes.

18. To recover from Accellion for these harms, Plaintiff and the Classes seek damages in an amount to be determined at trial, declaratory judgment, and injunctive relief requiring Accellion to: (1) disclose, expeditiously, the full nature of the Data Breach, the institutional clients affected, and the types of PII and PMI accessed, obtained, or exposed by the hackers; (2) implement improved data security practices to reasonably guard against future breaches of PII and PMI; and (3) provide, at its own expense, all impacted victims with lifetime identity theft protection services.

PARTIES

19. Plaintiff Valerie Whittaker is an adult individual who at all relevant times has been a citizen and resident of the State of Michigan. Plaintiff has used Kroger's pharmacy in Michigan on a continuous basis starting in approximately 2008 through present.

20. Plaintiff entrusted Kroger with her sensitive PII and PMI, including but not limited to her name, address, social security number, driver's license number, and medical information.

21. In February 2020, Plaintiff learned of the Data Breach, that Kroger used Accellion as a third-party vender, and that as a result of that relationship, Plaintiff's PII and PMI information, may have been accessed or exposed to unknown, unauthorized third parties during the Data Breach. Since the Data Breach, Plaintiff's has experienced potential fraud on her bank account whereby an unauthorized individual attempted to take out a loan in her name.

22. In response to the Data Breach, Plaintiff has spent hours to determine the extent of the disclosure of her PII and PMI, closely monitoring her credit, financial accounts, email and other accounts. Plaintiff has additionally spent hours communicating with her bank to further secure her financial accounts and monitor her PII and PMI.

23. Defendant, Accellion, Inc., is a Delaware corporation in the business of cloud-based file transfer solutions with its principal place of business in Palo Alto, California. Defendant is a citizen of California.

JURISDICTION AND VENUE

24. This Court has jurisdiction over this action pursuant to 28 U.S.C. §1332(d)(2)(A), as modified by the Class Action Fairness Act of 2005, because Plaintiff and at least one member of each of the Classes, as defined below, is a citizen of a different state than Defendant, there are more than 100 members of each of the Classes, and the aggregate amount in controversy exceeds $5,000,000 exclusive of interests and costs.

25. This Court has personal jurisdiction over Defendant because it is headquartered in and is a citizen of the State of California.

26. Venue is proper in this District, pursuant to 28 U.S.C. § 1391(b)(1), because a substantial part of the acts, omissions, and events giving rise to Plaintiff's claims occurred in this District. Further, Defendant resides in this District and is a resident of California.

FACTUAL BACKGROUND

Background of Accellion's Business Model

27. Accellion advertises itself as a defense to data breaches, stating: "[t]he Accellion enterprise content firewall prevents data breaches and compliance violations from third party cyber risk."[4] "With on-premise, private cloud, hybrid and FedRAMP deployment options, the Accellion content firewall provides the security and governance CISOs need to protect their organizations, mitigate risk, and adhere to rigorous compliance regulations."[5]

28. Accellion claims to have "protected more than 25 million end users at more than 3,000 global corporations and government agencies . . . ."[6]

29. Accellion recognizes that "[q]uality patient care requires accurate diagnosis, effective treatment, and bullet-proof data security."[7] Accellion markets its secure solutions to its healthcare clients, stating "[t]he Accellion enterprise content firewall allows hospitals and clinics, payers, and government health agencies to share X-rays, diagnoses, insurance information and other PHI securely and in compliance with patient privacy regulations like HIPAA, HITECH and GDPR."[8]

30. Accellion offers many different software solutions to its customers, including secure email, secure file sharing, secure mobile sharing, secure web forms, and secure managed file transfer.[9]

31. These programs perform a variety of functions, the most crucial being to share or transfer sensitive content in an easy and safe manner.

---

4 https://www.accellion.com/company/.

5 *Id.*

6 *Id.*

7 https://www.accellion.com/solutions/healthcare/.

8 *Id.*

9 https://www.accellion.com/platform/enterprise-content-firewall/.

32. In short, the very nature of Accellion's core business involves providing its clients with a way to securely share sensitive and private data, including the PII and PMI of the institutional clients' own clients, patients, and consumers.

33. Due to the very nature of its business, then, Accellion knew that its applications are and were used to transfer sensitive PII and PMI and as a result, that Accellion's software posed an attractive target for cybercriminals.

34. As a result, Accellion knows that its customers, and the individuals whose PII and PMI is stored or transferred using Accellion products, must rely on Accellion to ensure that its software is protected from outside attack.

35. Accellion refers to FTA as "Accellion's 20 year old legacy product," and has scheduled an "end of life" date for FTA on April 30, 2021.[10]

36. Accellion knew that maintenance of FTA's underlying operating system, CentOS 6, ended on November 30, 2020, which would limit Accellion's "ability to support the FTA software."[11]

37. Despite Accellion's knowledge that it could no longer fully support FTA, after November 30, 2020, Accellion was aware that many of its clients continued to use FTA in December 2020 and January 2021.

The Data Breach and Public Disclosure

38. On December 16, 2020, FTA triggered a built-in anomaly detector on one of Accellion's client's devices.[12]

[10] https://www.accellion.com/sites/default/files/resources/fta-eol.pdf (last accessed March 4, 2021).

[11] *Id.*

[12] Mandiant (FireEye, Inc.), *Accellion, Inc. File Transfer Appliance Security Assessment*, at 5–6 (Mar. 1, 2021), *available at* https://www.accellion.com/sites/default/files/trust-center/accellion-fta-attack-mandiant-report-full.pdf (hereinafter, Mandiant Report).

39. From December 16 to 19, 2020, Defendant investigated the anomaly and detected the vulnerabilities affecting Accellion FTA - 9.12.370 – SQL Injection (CVE-2021-27101) and OS Command Execution (CVE-2021-27104).[13]

40. On December 20 and 23, 2020, Defendant released two patches: FTA 9.12.380 and FTA 9.12.411, respectively, to remedy the vulnerabilities.[14]

41. Attacks on the FTA software continued into January, 2021, however.[15]

42. Accellion experienced a second exploit on January 20, 2021, and became aware of it on January 22, 2021, through multiple customer service inquiries.[16] In response, Accellion issued a critical security alert advising its FTA customers to shut down their FTA system immediately.[17]

43. From January 22 to 25, 2021, Defendant investigated the new exploits and identified two more vulnerabilities – Server-Side Request Forgery (CVE-2021-27103) and OS Command Execution (CVE-2021-27102).[18]

44. On January 25th and 28th, Defendant released patches FTA 9.12.416 and FTA_9.12.432, respectively, to remediate the vulnerabilities.[19]

45. In Accellion's initial public statement disclosing the Data Breach, it indicated that less than 50 clients were affected.[20]

46. In announcing that the December fix did not completely contain the Data Breach, Accellion stated: "This initial incident was the beginning of a concerted cyberattack on the

---

13 *Id.* at 6.

14 *Id.* at 5, 8–9.

15 *Id.* at 7.

16 *Id.* at 5, 7.

17 *Id.* at 5.

18 *Id.*

19 *Id.*

20 https://gizmodo.com/the-accellion-data-breach-seems-to-be-getting-bigger-1846250357.

Accellion FTA product that continued into January 2021. Accellion identified additional exploits in the ensuing weeks and rapidly developed and released patches to close each vulnerability."[21]

47. Kroger was notified of the Data Breach on January 23, 2021, at which point Kroger discontinued the use of Accellion's services.[22]

48. The University of Colorado, one of Accellion's higher-education clients affected by the Data Breach, puts the number of Accellion clients affected by the Data Breach at approximately 300.[23]

49. One governmental agency client of Accellion affected by the Data Breach, the Washington State Auditor's Office, has indicated that approximately 1.4 million individuals who filed unemployment insurance claims in 2020 were at risk of having their PII exposed in this Data Breach.[24]

50. News reports indicate that other major Accellion clients have also confirmed that they have been affected by Data Breach. These clients include the law firm Jones Day,[25] Singapore telephone company Singtel,[26] the Reserve Bank of New Zealand,[27] and the Australian Securities and Investments Commission.[28]

51. Kroger believes the following information, which includes Plaintiff's information, has been involved in the Data Breach:[29]

---

[21] https://www.accellion.com/company/press-releases/accellion-provides-update-to-recent-fta-security-incident/.

[22] https://www.kroger.com/i/accellion-incident.

[23] https://gizmodo.com/the-accellion-data-breach-seems-to-be-getting-bigger-1846250357.

[24] https://www.databreachtoday.com/washington-state-breach-tied-to-accellion-vulnerability-a-15909.

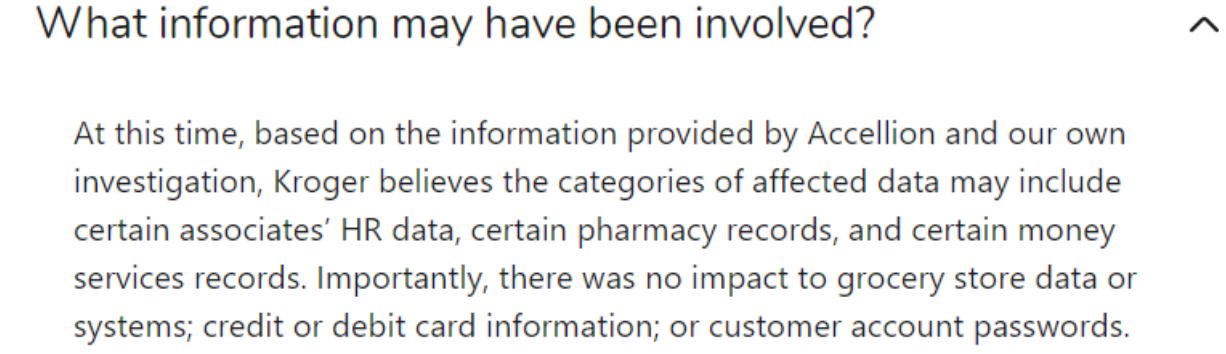
[25] https://news.bloomberglaw.com/business-and-practice/jones-day-hit-by-data-breach-as-vendor-accellion-hacks-widen.

[26] https://www.singtel.com/personal/support/about-accellion-security-incident.

[27] https://www.bankinfosecurity.com/nz-reserve-bank-issues-update-on-accellion-breach-a-16008.

[28] https://www.securityweek.com/australian-corporate-regulator-discloses-breach-involving-accellion-software.

[29] *Id.*



52. The total number of institutional clients and individual clients affected by the Data Breach is unknown.

53. Public reports indicate that the perpetrators of the Data Breach are using the stolen data to perpetrate extortion schemes, and threatened to publish or have already published stolen data on publicly-accessible websites.

54. According to Accellion's forensic investigator, Mandiant/FireEye, following the FTA exploits, several of Accellion's impacted clients received extortion threats in which the extortionists threaten to publish stolen data if their demands are not met.[30]

Accellion Knew the Risks of Attacks on FTA and that Harm to Consumers Would Result

55. At all relevant times, Accellion knew its FTA product was used for transferring valuable, sensitive PII and PMI and that as a result, Accellion's software would be attractive targets for cybercriminals.

56. Accellion also knew that any exploitation of its FTA software, and exposure of the information transferred using FTA, would result in the increased risk of identity theft and fraud against the individuals whose PII and PMI was compromised.

57. These risks are not merely theoretical; in recent years, numerous high-profile breaches have occurred at businesses such as Equifax, Yahoo, Marriott, Anthem, and many others.

[30] Andrew Moore, Genevieve Stark, Isif Ibrahima, Van Ta, Kimberly Goody, FireEye Threat Research Blog, *Cyber Criminals Exploit Accellion FTA for Data Theft and Extortion*, Feb. 22, 2021, *available at* https://www.fireeye.com/blog/threat-research/2021/02/accellion-fta-exploited-for-data-theft-and-extortion.html.

58. PII and PMI has considerable value and constitutes an enticing and well-known target to hackers. Hackers easily can sell stolen data as a result of the "proliferation of open and anonymous cybercrime forums on the Dark Web that serve as a bustling marketplace for such commerce."[31]

59. The prevalence of data breaches and identity theft has increased dramatically in recent years, accompanied by a parallel and growing economic drain on individuals, businesses, and government entities in the U.S. According to the Identity Theft Resource Center, in 2019, there were 1,473 reported data breaches in the United States, exposing 164 million sensitive records and 705 million "non-sensitive" records.[32]

60. In tandem with the increase in data breaches, the rate of identity theft and the resulting losses has also increased over the past few years. For instance, in 2018, 14.4 million people were victims of some form of identity fraud, and 3.3 million people suffered unrecouped losses from identity theft, nearly three times as many as in 2016. And these out-of-pocket losses more than doubled from 2016 to $1.7 billion in 2018.[33]

61. Even if stolen PII does not include financial or payment card account information, that does not mean there has been no harm, or that the breach does not cause a substantial risk of identity theft. Freshly stolen information can be used with success against victims in specifically targeted efforts to commit identity theft known as social engineering or spear phishing. In these forms of attack, the criminal uses the previously obtained PII about the individual, such as name, address, email address, and affiliations, to gain trust and increase the likelihood that a victim will be deceived into providing the criminal with additional information.

62. Stolen names and email addresses can also facilitate attacks known as "credential stuffing," where the attacker, armed with a known valid email address, can attempt to log-in to

---

[31] Brian Krebs, *The Value of a Hacked Company*, Krebs on Security (July 14, 2016), http://krebsonsecurity.com/2016/07/the-value-of-a-hacked-company/.

[32] *Data Breach Reports: 2019 End of Year Report*, IDENTITY THEFT RESOURCE CENTER, at 2, *available at* https://notified.idtheftcenter.org/s/resource#annualReportSection.

[33] Insurance Information Institute, *Facts + Statistics: Identity theft and cybercrime*, available at https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime#Identity%20Theft%20And%20Fraud%20Reports,%202015-2019%20(1) (last accessed March 1, 2021).

online accounts using the common formulas for usernames (email address, first initial and last name, or full name) and common passwords, or use software to mount a brute-force attack (guessing many passwords in rapid succession) against weak login portals.

Plaintiff and Class Members Suffered Damages

63. For the reasons mentioned above, Accellion's negligence, which allowed the Data Breach to occur, caused Plaintiff and members of the Classes significant injuries and harm in several ways. Plaintiff and members of the Classes must immediately devote time, energy, and money to: (1) closely monitor their credit, financial accounts, email and other accounts; (2) change login and password information on any sensitive account even more frequently than they already do; (3) more carefully screen and scrutinize phone calls, emails, and other communications to ensure that they are not being targeted in a social engineering or spear phishing attack; (4) search for suitable identity theft protection and credit monitoring services, and pay to procure them.

64. Once PII or PMI is exposed, there is virtually no way to ensure that the exposed information has been fully recovered or contained against future misuse. For this reason, Plaintiff and Class members will need to maintain these heightened measures for years, and possibly their entire lives, as a result of Accellion's negligence.

65. Plaintiff and Class members are also at a continued risk to the extent their PII or PMI continues to be stored in or transferred using Accellion's systems, which have already been shown to be susceptible to compromise and attack.

CLASS ALLEGATIONS

66. Plaintiff brings this case individually and, pursuant to Rule 23 of the Federal Rules of Civil Procedure, on behalf of the following classes:

The PII Class

> All individuals in the United States and its territories whose PII was compromised in the Accellion data breach which occurred starting in December 2020 (the "PII Class").

The PMI Class

> All individuals in the United States and its territories whose PMI was compromised in the Accellion data breach which occurred starting in December 2020 (the "PMI Class").

67. Excluded from the Classes are Defendant, its subsidiaries and affiliates, its officers, directors and members of their immediate families and any entity in which Defendant has a controlling interest, the legal representative, heirs, successors, or assigns of any such excluded party, the judicial officer(s) to whom this action is assigned, and the members of their immediate families.

68. Plaintiff reserves the right to modify or amend the definition of the proposed Classes prior to moving for class certification.

69. The requirements of Rule 23(a)(1) are satisfied. The Classes described above are so numerous that joinder of all individual members in one action would be impracticable. The disposition of the individual claims of the respective Class members through this class action will benefit both the parties and this Court. The exact size of the Classes and the identities of the individual members thereof are ascertainable through Defendant's records, including but not limited to, the files implicated in the Data Breach, but based on public information, the Classes include millions of individuals.

70. The requirements of Rule 23(a)(2) are satisfied. There is a well-defined community of interest and there are common questions of fact and law affecting members of the Classes. The questions of fact and law common to the Classes predominate over questions which may affect individual members and include the following:

a. Whether Defendant had a duty to protect the PII and PMI of Plaintiff and Class Members;

b. Whether Defendant's failure to adequately secure its software used to transfer Plaintiff's and the Classes' PMI violated CMIA;

c. Whether Defendant was negligent in failing to protect Plaintiff's and Class Members' PII and PMI, and breached its duties thereby;

d. Whether Plaintiff and Class Members are entitled to damages as a result of Defendant's wrongful conduct;

e. Whether Plaintiff and Class Members are third-party beneficiaries of contracts between Defendant and its Accellion FTA customers;

f. Whether Defendant breached the contracts with its Accellion FTA customers and thereby damaged Plaintiff and Class Members;

g. Whether Plaintiff and Class Members are entitled to restitution as a result of Defendant's wrongful conduct; and

h. Whether Defendant's conduct violated Cal. Bus. & Prof. Code § 17200, *et seq.*;

i. Whether Plaintiff and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Data Breach.

71. The requirements of Rule 23(a)(3) are satisfied. Plaintiff's claims are typical of the claims of the members of the Classes. The claims of the Plaintiff and members of the Classes are based on the same legal theories and arise from the same failure by Defendant to safeguard PII and PMI.

72. Plaintiff and members of the Classes were each consumers who had relationships with organizations that were clients of Accellion, and Plaintiff and members of the Classes all suffered harm when their PII and/or PMI was accessed and copied by an unauthorized third party.

73. The requirements of Rule 23(a)(4) are satisfied. Plaintiff is an adequate representative of the Classes because her interests do not conflict with the interests of the members of the Classes. Plaintiff will fairly, adequately, and vigorously represent and protect the interests of the members of the Classes and has no interests antagonistic to the members of the Classes. In addition, Plaintiff has retained counsel who are competent and experienced in the prosecution of class action litigation. The claims of Plaintiff and the Class members are substantially identical as explained above.

74. The requirements of Rule 23(b)(3) are satisfied here because a class action is the superior method of litigating these issues, and common issues will predominate. While the aggregate damages that may be awarded to the members of the Classes are likely to be substantial, the damages suffered by the individual members of the Classes are relatively small. As a result, the expense and burden of individual litigation make it economically infeasible and procedurally impracticable for each member of the Classes to individually seek redress for the wrongs done to them. Certifying the case as a Class will centralize these substantially identical claims in a single

proceeding, which is the most manageable litigation method available to Plaintiff and the Classes and will conserve the resources of the parties and the court system, while protecting the rights of each member of the Classes. Defendant's uniform conduct is generally applicable to the Classes as a whole, making relief appropriate with respect to each Class member.

CALIFORNIA LAW APPLIES TO THE ENTIRE CLASS

75. California's substantive laws apply to each member of the Classes, regardless of where in the United States the Class member resides. California's substantive laws may be constitutionally applied to the claims of Plaintiff and the Classes under the Due Process Clause, 14th Amend. §1, and the Full Faith and Credit Clause, Art. IV §1 of the U.S. Constitution. California has significant contact, or significant aggregation of contacts, to the claims asserted by Plaintiff and all Class members, thereby creating state interests that ensure that the choice of California state law is not arbitrary or unfair.

76. Defendant's U.S. headquarters and principal places of business are located in California. Defendant also owns property and conducts substantial business in California, and therefore California has an interest in regulating Defendant's conduct under its laws. Defendant's decision to reside in California and avail itself of California's laws, and to engage in the challenged conduct from and emanating out of California, renders the application of California law to the claims herein constitutionally permissible.

77. California is also the state from which Defendant's alleged misconduct emanated. This conduct similarly injured and affected Plaintiff and all other Class members.

78. The application of California laws to the Classes is also appropriate under California's choice of law rules because California has significant contacts to the claims of Plaintiff and the proposed Classes, and California has a greater interest in applying its laws here than any other interested state.

FIRST CAUSE OF ACTION
NEGLIGENCE
(On Behalf of Plaintiff and the Classes)

79. Plaintiff restates and realleges all proceeding allegations above as if fully set forth herein.

80. Accellion owed a duty under common law to Plaintiff and Class members to exercise reasonable care with respect to the PII and PMI stored or transferred using Accellion's software products and services.

81. Accellion's duty to use reasonable care arose from several sources, including but not limited to those described below.

82. Accellion had a common law duty to prevent foreseeable harm to others. This duty existed because Plaintiff and Class members were the foreseeable and probable victims of any inadequate security practices on the part of Defendant. By providing software products and services specifically designed for and marketed for the collection and transfer of valuable PII and PMI, Accellion was obligated to act with reasonable care to protect against these foreseeable threats.

83. Accellion's duty also arose from Accellion's position as a data services vendor to healthcare, educational, and other organizations. Accellion knows and intends that its software will be used for collection, storage, and transfer of highly sensitive information. Consumers generally have no knowledge that Accellion's software will be used for the transmission of their PII or PMI, and therefore do not have the opportunity to consent to or "opt out" of Accellion's involvement.

84. Accellion holds itself out as a trusted provider of software to be used in the collection, storage, and transfer of sensitive data, and thereby assumes a duty to reasonably protect that data. Because of its role as a cloud computing and file transfer vendor to a large number of organizations, Accellion was in a unique and superior position to protect against the harm suffered by Plaintiff and Class members as a result of the Data Breach.

85. Accellion breached the duties owed to Plaintiff and Class members and thus was negligent. Accellion breached these duties by, among other things: (a) mismanaging its software and failing to identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of sensitive information that resulted in the unauthorized access and compromise of PII and PMI; (b) allowing clients to continue utilizing the outdated FTA software for sensitive file transfers after Accellion knew that FTA could no longer be fully maintained and supported in accordance with modern security standards; (c) failing to design and implement information safeguards to control these risks; (d) failing to adequately test and monitor the effectiveness of the safeguards' key controls, systems, and procedures; (e) failing to evaluate and adjust its information security program in light of the circumstances alleged herein; and (f) failing to detect the breach at the time it began or within a reasonable time thereafter.

86. But for Accellion's wrongful and negligent breach of its duties owed to Plaintiff and Class members, their PII and PMI would not have been compromised.

87. As a direct and proximate result of Accellion's negligence, Plaintiff and Class members have suffered injuries, including:

a. Theft and exposure of their PII and/or PMI;

b. Costs associated with requested credit freezes;

c. Costs associated with the detection and prevention of identity theft and unauthorized use of the financial accounts;

d. Costs associated with purchasing credit monitoring and identity theft protection services;

e. Unauthorized charges and loss of use of and access to their financial account funds and costs associated with inability to obtain money from their accounts or being limited in the amount of money they were permitted to obtain from their accounts, including missed payments on bills and loans, late charges and fees, and adverse effects of their credit;

f. Lowered credit scores resulting from credit inquiries following fraudulent activities;

g. Costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Accellion Data Breach – including finding fraudulent charges, cancelling and reissuing cards, enrolling in credit monitoring and identity theft protection services, freezing and unfreezing accounts, and imposing withdrawal and purchase limits on compromised accounts;

h. The imminent and certainly impending injury flowing from the increased risk of potential fraud and identity theft posed by their PII and/or PMI being placed in the hands of criminals;

i. Damages to and diminution in value of their PII and/or PMI entrusted, directly or indirectly, to Accellion; and

j. Continued risk of exposure to hackers and thieves of their PII and/or PMI, which continues to be stored and transferred using Accellion's software and is subject to further breaches so long as Accellion fails to undertake appropriate and adequate measures to protected Plaintiff and Class members.

88. As a direct and proximate result of Accellion's negligence, Plaintiff and Class members are entitled to damages, including compensatory, punitive, and/or nominal damages, in an amount to be proven at trial.

SECOND CAUSE OF ACTION
NEGLIGENCE PER SE
(On Behalf of Plaintiff and the Classes)

89. Plaintiff restates and realleges all proceeding factual allegations above as if fully set forth herein.

90. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce" including, as interpreted and enforced by the FTC, the unfair act or practice by companies such as Accellion or failing to use reasonable measures to protect PII and PMI. Various FTC publications and orders also form the basis of Accellion's duty.

91. Pursuant to the CMIA, Defendant had a duty to implement safeguards to protect Plaintiff's and the Class members' PMI.

92. Accellion violated Section 5 of the FTC Act (and similar state statutes) and the CMIA by failing to use reasonable measures to protect PII and PMI and not complying with the industry standards. Accellion's conduct was particularly unreasonable given the nature and amount of PII and PMI it obtained and stored and the foreseeable consequences of a data breach involving PII and PMI of organizations' patients, clients, and consumers.

93. Accellion's violation of Section 5 of the FTC Act (and similar state statutes) and the CMIA constitutes negligence *per se*.

94. Plaintiff and members of the Classes are consumers within the class of persons Section 5 of the FTC Act (and similar state statutes) was intended to protect.

95. Plaintiff and members of the PMI Class are patients within the class of persons CMIA was intended to protect.

96. Moreover, the harm that has occurred is the type of harm that the FTC Act (and similar state statutes) and CMIA was intended to guard against. Indeed, the FTC has brought dozens of enforcement actions against businesses which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm suffered by Plaintiff and Class members.

97. As a direct and proximate result of Accellion's negligence, Plaintiff and Class members have been injured as described herein, and are entitled to damages, including compensatory, punitive, and nominal damages, in an amount to be proven at trial.

THIRD CAUSE OF ACTION
THIRD PARTY BENEFICIARY CLAIM
(On Behalf of Plaintiff and the Classes)

98. Plaintiff restates and realleges all proceeding allegations above as if fully set forth herein.

99. Accellion entered into contracts directly with its clients, including Kroger, to provide them with Accellion FTA.

100. Defendant purported that Accellion FTA would provide a convenient and secure solution for its clients to transfer and store PII and PMI.

101. Although Plaintiff and members of the Classes were not a direct party to the Accellion FTA services contract, part of the purpose of the contract was to securely transfer and store PII and/or PMI belonging to Plaintiff and members of the Classes.

102. According to Defendant's own marketing, Defendant knew, or should have known, that the PII and PMI that it transferred and stored on behalf of its clients needed to be transferred and stored securely.

103. Defendant knew or should have known that its clients, including Kroger, would use Accellion FTA as advertised to transfer and store Plaintiff's and members of the Classes PII and/or PMI.

104. Defendant breached the contract with its clients, including Kroger, by failing to maintain the PII and PMI secure and confidential.

105. As a result of Accellion's wrongful conduct as alleged in this Complaint (including among other things its utter failure to employ adequate data security measures, its continued maintenance and use of the PII and PMI belonging to Plaintiff and Class members without having adequate data security measures, and its other conduct facilitating the theft of that PII and PMI), Plaintiff and Class members have suffered and continue to suffer harm.

FOURTH CAUSE OF ACTION
CALIFORNIA CONFIDENTIALITY OF MEDICAL INFORMATION ACT, Cal. Civ. Code §6, *et seq.*
(On Behalf of Plaintiff and the PMI Class)

106. Plaintiff restates and realleges all proceeding allegations above as if fully set forth herein.

107. Defendant is a "provider of health care" as defined in Cal. Civ. Code §56.06, and is therefore subject to the requirements of the CMIA, Cal. Civ. Code §§56.10(a) and (d), 56.35, 56.36(b), 56.101(a) and (b).

108. Defendant is organized in part for the purpose of maintaining medical information in order to make that information available to an individual or provider of health care, for purposes of information management, diagnosis, or treatment, and is therefore a "provider of health care" under the CMIA.

109. Plaintiff and the PMI Class members are "patients," as defined in CMIA, Cal. Civ. Code §56.06(k), as they are "natural person[s], whether or not still living, who received health care services from a provider of health care and to whom medical information pertains."

110. Defendant disclosed "medical information," as defined in CMIA, Cal. Civ. Code §56.05(j), to unauthorized persons without first obtaining consent, in violation of Cal. Civ. Code §56.10(a).

111. Defendant's negligence resulted in the release of individually identifiable medical information pertaining to Plaintiff and the PMI Class to unauthorized persons and the breach of the confidentiality of that information. Defendant's negligent failure to maintain, preserve, store, abandon, destroy, and/or dispose of Plaintiff's and PMI Class members' medical information in a manner that preserved the confidentiality of the information contained therein, in violation of the CMIA.

112. Defendant's computer systems did not protect and preserve the integrity of electronic medical information in violation of Cal. Civ. Code §56.101(b)(1)(A).

113. Plaintiff and members of the PMI Class were injured and have suffered damages, as described above, from Defendant's illegal disclosure and negligent release of their medical information in violation of Cal. Civ. Code §§56.10 and 56.101, and therefore seek relief under Civ. Code §§56.35 and 56.36, including actual damages, nominal statutory damages of $1,000, punitive damages of $3,000, injunctive relief, and attorney fees, expenses and costs.

FIFTH CAUSE OF ACTION
UNLAWFUL AND UNFAIR BUSINESS PRACTICES
Cal. Bus. & Prof. Code §17200, *et seq.*
(On Behalf of Plaintiff and the Classes)

114. Plaintiff restates and realleges all proceeding allegations above as if fully set forth herein.

115. Defendant's conduct has violated and continues to violate the California Unfair Competition Law ("UCL"), Cal. Bus. & Prof. Code §17200, *et seq.*, which prohibits unlawful, unfair, or fraudulent business acts or practices.

116. Defendant's conduct of violating the CMIA and Section 5 of the FTC Act is unlawful under the UCL.

117. Defendant's conduct of violating the CMIA and Section 5 of the FTC Act also constitutes unfair conduct under the UCL.

118. Accellion violated Section 5 of the FTC Act (and similar state statutes) and the CMIA by failing to use reasonable measures to protect PII and PMI and not complying with the industry standards. Accellion's conduct was particularly unreasonable given the nature and amount of PII and PMI it obtained and stored and the foreseeable consequences of a data breach involving PII and PMI of organizations' patients, clients, and consumers.

119. Defendant disclosed "medical information," as defined in CMIA, Cal. Civ. Code §56.05(j), to unauthorized persons without first obtaining consent, in violation of CMIA.

120. Had Defendant complied with the FTC Act and CMIA, Plaintiff and members of the Classes would not have suffered, or continue to suffer, from the harm alleged herein.

121. Defendant's conduct and use of an admittedly outdated product constitutes an unfair business practice by failing to provide adequate security measures to prevent hackers from causing the Data Breach and causing substantial harm and impending risk of identity theft and fraud to Plaintiff and members of the Classes.

122. Defendant's unfair practices substantially outweigh the potential benefits gained from those practices. This is bolstered by the fact that there were reasonable alternatives available to Defendant.

123. As a result of Accellion's wrongful conduct as alleged in this Complaint (including among other things its utter failure to employ adequate data security measures, its continued maintenance and use of the PII and PMI belonging to Plaintiff and Class members without having adequate data security measures, and its other conduct facilitating the theft of that PII and PMI), Plaintiff and Class members have suffered and continue to suffer harm.

124. Plaintiff and members of the Classes are entitled to restitution and equitable relief as a result of Defendant's conduct.

SIXTH CAUSE OF ACTION
Violation of California Consumer Privacy Act, Cal. Civ. Code §1798.100 *et seq*.
(On Behalf of Plaintiff and the Classes)

125. Plaintiff restates and realleges all proceeding allegations above as if fully set forth herein.

126. The California Consumer Privacy Act ("CCPA") protects consumers' personal information from collection and use by businesses without consumers' notice and consent.

127. Pursuant to Civil Code section 1798.150(a)(1), a private right of action for civil remedies is available to "[a]ny consumer whose nonencrypted and nonredacted personal information, as defined in subparagraph (A) of paragraph (1) of subdivision (d) of Section 1798.81.5, is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business's violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information." "Personal information" as defined by Civil Code Section 1798.81.5(d)(1)(A)(vi) includes an individual's first name or first initial and the individual's last name in combination with unique biometric data generated from measurements or technical analysis of human body characteristics, such as a fingerprint, retina, or iris image, used to authenticate a specific individual, when either the name or the data elements are not encrypted or redacted.

128. In violation of the CCPA, Accellion caused third parties to access and exfiltrate without authorization and failed to prevent Plaintiff's information from unauthorized disclosure as a result of Accellion's of its duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information of Plaintiff and Class members.

129. Civil Code section 1798.150(a)(1)(A)-(C) provides that consumers whose personal information is subject to unauthorized access or disclosure may institute a civil action for any of the following: (A) To recover damages in an amount not less than $100 and not greater than $750 per consumer per incident or actual damages, whichever is greater; (B) Injunctive or declaratory relief; (C) Any other relief the court deems proper.

SEVENTH CAUSE OF ACTION
Request for Relief under the Declaratory Judgment Act
28 U.S.C. §2201 *et seq*.
(On Behalf of Plaintiff and the Classes)

130. Plaintiff restates and realleges all proceeding allegations above as if fully set forth herein.

131. Under the Declaratory Judgment Act, 28 U.S.C. §2201 *et seq*., this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief.

132. Furthermore, the Court has broad authority to restrain acts, such as here, that are tortious and that violate the terms of the federal and state statutes described in this complaint.

133. An actual controversy has arisen in the wake of the Data Breach regarding its common law and other duties to properly maintain and protect Plaintiff's PII and PMI as alleged herein in violation of Defendant's common law and statutory duties.

134. Plaintiff alleges that Defendant's data security measures were inadequate and remain inadequate. Furthermore, Defendant continues to suffer injury and damages as described herein.

135. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. Defendant continues to owe a legal duty to act reasonably in managing and securing PII and PMI under, *inter alia*, the common law, and various state statutes referred to herein;

b. Defendant continues to breach its legal duty by actively mishandling Plaintiff's and the Classes' data and failing to employ reasonable measures to secure PII and PMI; and

c. Defendant's ongoing breaches of their legal duties continue to cause Plaintiff and the Classes harm.

136. The Court should also issue corresponding injunctive relief, including but not limited to, enjoining Defendant from engaging in the unlawful conduct alleged herein and to

implement functionality sufficient to prevent unauthorized collection and use of PII and PMI in the future, and other appropriate equitable relief, including but not limited to, improving its privacy data security measures.

137. If an injunction is not issued, Plaintiff will suffer irreparable injury and lack an adequate legal remedy in the event of Defendant's ongoing conduct.

138. State laws require the protection of Plaintiff's and the Classes' PII and PMI.

139. The risk of continued violations of law is real, immediate, and substantial. Plaintiff does not have an adequate remedy at law because many of the resulting injuries are reoccurring and Plaintiff will be forced to bring multiple lawsuits to rectify the same conduct.

140. The hardship to Plaintiff and the Classes if an injunction is not issued exceeds the hardship to Defendant if an injunction is issued. On the other hand, the cost to Defendant of complying with an injunction by complying with law and by ceasing to engage in the misconduct alleged herein is relatively minimal, and Defendant has a pre-existing legal obligation to protect Plaintiff's and the Classes' PII and PMI.

141. Issuance of the requested injunction will serve the public interest by preventing another data breach at Accellion, thus eliminating the injuries that would result to Plaintiff, the Classes, and the potentially tens of thousands of consumers whose PII and PMI would be compromised.

PRAYER FOR RELIEF

WHEREFORE Plaintiff on behalf of herself and all other similarly situated, prays for relief as follows:

A. For an order certifying the Class under Rule 23 of the Federal Rules of Civil Procedure and naming Plaintiff as representative of the Classes and Plaintiff's attorneys as Class Counsel to represent the Classes;

B. For an order finding in favor of Plaintiff and the Classes on all counts asserted herein;

C. For damages in an amount to be determined by the trier of fact;

D. For an order of restitution and all other forms of equitable monetary relief;

E. Declaratory and injunctive relief as described herein;

F. Awarding Plaintiff's reasonable attorneys' fees, costs, and expenses;

G. Awarding pre- and post-judgment interest on any amounts awarded; and,

H. Awarding such other and further relief as may be just and proper.

JURY TRIAL DEMAND

A jury trial is demanded on all claims so triable.

Dated: March 11, 2021

Respectfully submitted,

SCOTT+SCOTT ATTORNEYS AT LAW LLP

s/ *Alex. M. Outwater*

Alex M. Outwater (CA 259062)
600 W. Broadway, Suite 3300
San Diego, CA 92101
Telephone: 619-233-4565
Facsimile: 619-233-0508
aoutwater@scott-scott.com

SCOTT+SCOTT ATTORNEYS AT LAW LLP
Joseph P. Guglielmo (*pro hac vice forthcoming*)
Erin Green Comite (*pro hac vice forthcoming*)
Carey Alexander (*pro hac vice forthcoming*)
230 Park Avenue, 17th Floor
New York, NY 10169
Telephone: 212-223-6444
Facsimile: 212-223-6334
jguglielmo@scott-scott.com
ecomite@scott-scott.com
calexander@scott-scott.com

Attorneys for Valerie Whittaker